Référentiel de certification et évaluation

Analyser les incidents de sécurité informatique

Mars 2024

<table>
<tr><td rowspan="2">REFERENTIEL DE COMPETENCES
Identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d’activités</td><td colspan="2">REFERENTIEL D’EVALUATION
Définit les critères et les modalités d'évaluation des acquis</td></tr>
<tr><td>MODALITES D’EVALUATION</td><td>CRITÈRES D'ÉVALUATION</td></tr>
<tr><td>C1. Détecter les activités suspectes depuis la console d’un système de gestion des événements et des informations de sécurité (SIEM*), en analysant les événements collectés afin de signaler les incidents de sécurité redoutés.</td><td rowspan="2">E1. Mise en situation professionnelle (C1, C2, C3, C4, C5)
L’évaluation se fait dans un contexte de projet de sécurisation d’un système d’information, réel ou fictif, avec une politique de sécurité établie.
Le candidat est partie prenante de l’activité de surveillance avec un rôle d’expert technique, garant de la méthodologie à suivre.
L’évaluation porte sur les étapes de détection et d’analyse des incidents et la mise en œuvre d’une veille professionnelle en cybersécurité.
<u>Livrable</u> :
- rapport professionnel individuel,
<u>Évaluation</u> :
- correction du rapport professionnel,</td><td>- L’objectif de la surveillance est rappelé;

- Les événements en lien avec l’objectif de surveillance sont repérés depuis la console du SIEM*;

- Les activités suspectes et les évidences associées sont identifiées;

- Des améliorations possibles sont formulées pour le filtrage des événements et la génération des alertes.</td></tr>
<tr><td>C2. Analyser une activité suspecte, en déterminant sa véracité et son niveau de gravité afin de déterminer la nature et le niveau de réponse à appliquer.</td><td>- La nature de l’activité et les évidences qui la rendent suspecte sont rappelées;

- Un mode opératoire est décrit pour la recherche et la validation</td></tr>
</table>

	- soutenance orale individuelle.	d'explications probables permettant de légitimer l'activité suspecte; - La nature de l'incident est spécifiée; - L'impact de l'incident sur le reste de l'activité est envisagé; - Des mesures d'urgence à prendre sont préconisées; - L'alerte incident est renseignée dans le respect de la politique de réponse à incident de sécurité (SIRP*);
C3. Identifier les tactiques, les techniques et l'objectif d'une attaque, en relevant son point de départ et les indicateurs de compromission pour appuyer la stratégie de réponse à un incident de sécurité.		- Les étapes de l'analyse de l'incident sont décrites et justifiées à partir des évidences collectées; - L'objectif de l'attaquant est identifié; - Le point de départ de l'attaque et sa nature sont décrits; - Les tactiques et les techniques de

		l'attaquant sont identifiées et décrites
C4. Rédiger un rapport d'incident en respectant la politique de réponse à incident de sécurité afin de soutenir l'effort de réponse et de remédiation du système d'information.		- Sont rappelés la procédure, le formalisme et l'outillage imposé par la politique de réponse à incident de sécurité pour la rédaction du rapport; - Le rapport contient les informations suivantes : - une description de l'incident; - les évidences et les éléments d'analyse permettant d'assurer la véracité de l'incident; - une évaluation de l'impact de l'incident; - les mesures d'urgence prises; - tous les éléments d'analyse de l'attaque; - les conséquences de l'incident; - une liste de préconisations cohérentes avec les causes de l'incident; - Le rapport respecte les exigences liées à la politique de réponse à incident de sécurité.

C5. Etablir un système de veille professionnelle en cybersécurité, en identifiant des sources de confiance, en les agrégeant à l'aide d'un outil dédié, en analysant les informations recueillies et en les partageant avec les parties prenantes du projet de sécurisation afin d'ajuster son système de défense, en continu, aux actualités et aux mises à jour critiques.		- Un objectif de veille est fixé, - Un cadre méthodologique et opérationnel (outils, supports, espaces d'échanges...) est défini pour la veille, - Des sources d'autorités sont choisies en priorité (OpenCVE, Cert-fr, Cert-eu...), elles sont identifiées et leur fiabilité évaluée, - Les opportunités de réinvestissement des informations et données collectées dans le cadre d'un projet de sécurisation d'un SI sont rappelées.

Glossaire

- **SIEM (*Security Information and Event Management* ou système de gestion des informations et des événements de sécurité)** : un système dédié à la surveillance des systèmes et réseaux informatiques. Un SIEM permet la collecte des données relatives aux activités informatiques sur les systèmes et réseaux sous surveillance, leur normalisation, leur agrégation, la recherche de corrélation, le reporting, l'archivage, le rejeu des événements.
- **SIRP (Security Incident Response Policy)** : une politique de réponse aux incidents de sécurité (SIRP) est un ensemble de processus et de procédures qu'une entreprise met en place pour détecter et répondre aux vulnérabilités et aux incidents de sécurité.